Reference: SEC/5/1 **02SEC015**

17 September 2001

INFORMATION PAPER

IFALPA SECURITY (SEC) COMMITTEE MEETING
TOKYO, JAPAN, 16-18 OCTOBER 2001

Agenda Item 2: UNLAWFUL INTERFERENCE

REVIEW OF SEC POLICIES FOLLOWING RECENT EVENTS
(Presented by Jo Puff, Chairman)

INTRODUCTION

This paper invites discussion by the Committee of measures to be employed in regard to the recent events.

BACKGROUND

- There is no 100% security in air travel. There will always be degree of risk, no matter how small it may be.
- The increase of security on board civil air transport aircraft is limited due to constraints from design, operation and environment.
- Security measures on the ground have to be designed so that criminal elements (hijackers) are prevented from boarding an aircraft.
- Aviation Security must be made redundant. A failure at one stage must be caught by another.
- Existing security regulations must be applied strictly.

DISCUSSION ITEMS

- Cockpit doors
- On Board Weapons
- Skymarshalls
- Video Monitoring of the Flight Deck and Cabin
- Remote Control of Aircraft
- Automatic GPWS
- Flight Schools and Training
- Manufacturers and Suppliers
- Use of Simulators by non-professionals (“fun flights”)
- Aircraft access and availability of aircraft manuals and logs
- Security in Communication and Data Transfer
- Review of hijack procedures
- Passive and active aircraft protection

1. COCKPIT DOORS

The following proposal for amendment to ICAO Annex 8 Part III is currently circulated for comment via State Letter AN 3/40-01/58:

> "11.2 Protection of flight crew compartment
> ***For commercial aeroplanes having passenger seating capacities greater than 30 and a maximum certified T.O. mass of 25 000 kg or more***, in all aeroplanes which are equipped with a flight crew compartment door, this door and the flight crew compartment bulkhead shall be designed to minimize penetration by small arms fire and grenade shrapnel."

IFALPA policy states:

> "**ENTRY TO FLIGHT DECK/LOCKING OF FLIGHT DECK DOOR**
> IFALPA strongly opposes the enforced locking of flight deck doors The locking of such doors should be at the discretion of the aircraft commander.
> NOTE: The enforced locking of flight deck doors is not considered to be a substitute for proper and adequate ground security and pre-boarding screening and control. The locking of such doors can reduce the safety of the crews and aircraft by denying access in the case of an accident or incident."
>
> *and*
>
> "**REINFORCEMENT OF COCKPIT WALLS AND DOOR**
> In respect of all future aircraft, the cockpit bulkhead and door should be constructed both to withstand small arms' fire and grenade shrapnel, as a protective measure in both hijacking and sabotage situations. The design should be in such a way that it does not hinder emergency operation."

Even armoured doors cannot prevent hijackers from forcing their entry into a cockpit, unless accepting the sacrifice of the life of cabin crew and passengers as a consequence.

In addition, most cockpits are not "self-contained" and require the cockpit crew to enter the cabin area for physiological and rest requirements.

2. ON BOARD WEAPONS

(Use of the Emergency Equipment as a weapon)

Many equipment items on board an aircraft can be used as a weapon, such as:

- On board tools
- Oxygen containers, fire extinguishers
- Crash axe, crash bars
- On board kitchen equipment
- Bottles and glasses

IFALPA policy states:

> "**EQUIPMENT OF FUTURE AIRCRAFT VIS A VIS SECURITY**
> The design and certification criteria to be applied to future aircraft should encompass both equipment and operational practices which would help to reduce the possibility of unlawful interference and to bring about the safe outcome of a hijacking/sabotage situation; such criteria should include the following:
>
> **STOWAGE OF WEAPONS AND OTHER SECURITY-REMOVED ITEMS**
> Provision should be made on all future aircraft for the secure transportation of passenger weapons and other security-removed items in such a manner that they are not accessible during flight, but are not necessarily placed haphazardly in the cargo hold.
>
> **STOWAGE OF FIRE AXES ON BOARD AIRCRAFT**
> Provision should be made on all aircraft for the stowage of fire axes in such a manner that they are accessible, but concealed."

3. SKYMARSHALLS

3.1 IFALPA objects to the use of armed guards on board aircraft.

IFALPA policy states:

> **"CARRIAGE OF ARMED GUARDS**
> IFALPA strongly opposes the use of armed guards aboard civil aircraft …. Their carriage hides the necessity for proper airport and aircraft security and increases the risk of the use of such firearms.
> Note: The installation of special security protection or provisions for cabin, flight deck and other sensitive areas of the aircraft is not considered to be a substitute for proper and adequate ground security and pre-board screening and control."

The risk from the use of firearms to crew and passengers cannot be calculated and it can also critically impact the pressurised cabin, electric and hydraulic control lines, and computer systems. Individuals using such firearms would be beyond the control of the aircraft Commander.

3.2 It seems feasible to envisage the employment of crew members (possibly as additional crew) which have been specially trained in security, including the de-escalation of airborne crisis situations. Note: crew members act under the authority of the aircraft Commander.

IFALPA policy states:

> **"TRAINING**
> Appropriate aviation personnel including all flight crew should receive both theoretical and practical confrontational management training for dealing with unruly and violent passengers."

4. VIDEO MONITORING OF THE FLIGHT DECK AND CABIN

Video monitoring of the flight deck will not assist in case of an unlawful interference.

Monitoring of the cabin can enable the aircraft Commander to assess a situation and could prevent a surprise escalation and cockpit intrusion.

(Video monitoring of other safety-relevant areas can also be beneficial, such as cargo holds, engines, flight controls and gear systems).

5. REMOTE CONTROL OF AIRCRAFT

Steering an aircraft remotely widens the possibility for unlawful interference without the need to even board the aircraft.

In addition, numerous technical and legal issues would have to be solved to command an aircraft remotely.

6. AUTOMATIC GPWS

A control system providing flight envelope protection from ground and obstacles, which automatically assumes control of the aircraft, could easily be deactivated after the aircraft has been brought on a collision course, either by deactivation of the equipment, by cutting off power or by shutting down the engines. In addition, malfunctions cannot be excluded.

7. FLIGHT SCHOOLS AND TRAINING

Each applicant for training should be security screened upon application at a flight school. Further screening at regular intervals should be considered.

8. MANUFACTURERS AND SUPPLIERS

Employees of companies and organisations dealing with compiling and providing flight and navigation data should be security screened. This includes dealing with the following data and services:

- terrain and obstacle data
- maps
- approach and departure procedures
- navigation data base (FMS/EGPWS)
- flight planning / dispatch (SITA/LIDO/ARINC)

Navigational data are to be classified and to be made available to authorised personnel only.

Navigational and other relevant data in commercial software (e.g. in PC simulator programmes) is to be altered so that the information cannot be used for actual flying.

9. USE OF SIMULATORS BY NON-PROFESSIONALS ("FUN FLIGHTS")

The use of aircraft simulators should be limited to aviation use only, such as training, checking, and research. Operators and users of flight simulators should be subject to security screening.

10. AIRCRAFT ACCESS AND AVAILABILITY OF AIRCRAFT MANUALS AND LOGS

Training und Flight Manuals should not be available to the general public. The same applies to route manuals and aeronautical information publications, including approach and departure procedures and aerodrome layouts.

Flight monitoring by unauthorised persons should not be allowed, e.g. via the Internet.

11. SECURITY IN COMMUNICATION AND DATA TRANSFER

Data systems without encryption (e.g. ACARS) should not be used to transfer operational or security relevant data such as:

- flight plans
- air traffic control clearances (e.g. pre-departure clearance)
- passenger manifest information
- load manifests

12. REVIEW OF HIJACK PROCEDURES

Current security measures must be examined with a view to the changed threat. Caution must be exercised when implementing radical changes, bearing in mind that existing provisions have proven practical and efficient under the test of time.

All Authorities must require security training for crew members which includes a comprehensive and detailed training syllabus. This training must have the full support by the airlines.

13. PASSIVE AND ACTIVE AIRCRAFT PROTECTION

ICAO Annex 8 includes Standards and recommendations regarding aircraft survivability including from damage by explosions or bullets, including the reinforcement (Kevlar) of the cockpit bulk head, electronics and avionics bays, and cargo holds.

The installation of chaffe / flares for protection from infra-red and laser guided surface-to-air missiles is feasible.